Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously Presented) A method for securing radio transmissions utilizing a conventional radio, said method comprising the steps of:

providing a conventional radio, said conventional radio being incapable of encrypting or decrypting signals, said radio including a conventional microphone port that is configured to be coupled to a conventional microphone and a conventional speaker port that is configured to be coupled to a conventional speaker, said radio remaining unmodified;

providing a computer system coupled between a microphone and said radio, wherein inputs into said radio are received first by said computer system, said computer system being separate and apart from said radio;

receiving, within said computer system, an input analog signal from said microphone;

encrypting, within said computer system, said input analog signal utilizing public key encryption to form an encrypted voice file;

passing said encrypted voice file from said computer system to said microphone port that is included within said unmodified radio; and

transmitting said encrypted voice file utilizing said unmodified radio, wherein radio transmissions from said radio are secured.

2. (Original) The method according to claim 1, further comprising the step of encrypting, within said computer system, said input analog signal utilizing a key pair, said key pair including a public key and a private key.

3. (Original) The method according to claim 2, further comprising the step of encrypting, within said computer system, said input analog signal utilizing said public key.

4. (Previously Presented) The method according to claim 1, wherein the receiving step comprises:

receiving, within a first application executing within said computer system, said input analog signal from said microphone;

wherein the encrypting step comprises encrypting, utilizing said first application, said input analog signal utilizing public key encryption to form said encrypted voice file;

wherein the passing step comprises passing said encrypted voice file from said first application to said microphone port of said unmodified radio.

5. (Currently Amended) The method according to claim 1, wherein the receiving step comprises:

converting, by a microphone driver that is executing within said computer system, said input analog signal to a file, said file being in a standard voice file format;

constantly monitoring, by ~~said~~ a first application, inputs received from said microphone; and

detecting, by said first application, a receipt of said file;

wherein the encryption step comprises in response to a detection by said first application of said receipt of said file, encrypting to form said encrypted voice file, by said first application utilizing a public key that is part of a public key/private key pair assigned to said computer system.

6. (Previously Presented) The method according to claim 1, further comprising the steps of:

providing a second conventional radio, said second conventional radio being incapable of encrypting or decrypting signals, said second radio including a second microphone port that is configured to be coupled to a second conventional microphone and a second speaker port that is configured to be coupled to a second conventional speaker, said second radio remaining unmodified;

providing a second computer system coupled between said second speaker and said second unmodified radio, wherein outputs from said second radio are received first by said second computer system before being output to said second speaker, said second computer system being separate and apart from said second radio;

receiving, within said second computer system, an encrypted output from said second speaker port included within said unmodified second radio;

decrypting, within said second computer system, said encrypted output utilizing public key encryption to form a decrypted output; and

outputting said decrypted output from said second computer system to said second speaker.

7. (Previously Presented) The method according to claim 6, wherein within said second computer system the step of receiving further comprises:

constantly monitoring, by a second application that is executing within said second computer system, said second speaker port;

receiving, by said second application, said encrypted output from said second speaker port;

wherein the decrypting step comprises decrypting, by said second application, said encrypted output utilizing public key encryption.

8. (Canceled)

9. (Previously Presented) The method according to claim 7, further comprising the steps of:

obtaining, by said second computer system, a private key of said computer system; and

wherein the decrypting step further comprises decrypting said encrypted output utilizing said private key.

10. (Previously Presented) The method according to claim 9, further comprising the step of exchanging said private key between said computer system and said second computer system prior to transmitting said encrypted voice file.

11. (Previously Presented) A system for securing radio transmissions utilizing a conventional radio, comprising:

a conventional radio, said conventional radio being incapable of encrypting or decrypting signals, said radio including a conventional microphone port that is configured to be coupled to a conventional microphone and a conventional speaker port that is configured to be coupled to a conventional speaker, said radio remaining unmodified;

a computer system coupled between a microphone and said radio, wherein inputs into said radio are received first by said computer system, said computer system being separate and apart from said radio;

said computer system for receiving an input analog signal from said microphone;

said computer system for encrypting said input analog signal utilizing public key encryption to form an encrypted voice file;

said computer system for passing said encrypted voice file from said computer system to said microphone port that is included within said unmodified radio; and

said unmodified radio for transmitting said encrypted voice file, wherein radio transmissions from said radio are secured.

12. (Original) The system according to claim 11, further comprising said computer system for encrypting said input analog signal utilizing a key pair, said key pair including a public key and a private key.

13. (Original) The system according to claim 12, further comprising said computer system for encrypting said input analog signal utilizing said public key.

14. (Previously Presented) The system according to claim 11, said computer system for receiving further comprising:

a first application executing within said computer system for receiving said input analog signal from said microphone;

said computer system for passing said encrypted further comprises said first application for encrypting said input analog signal utilizing public key encryption to form said encrypted voice file and passing said encrypted voice file from said first application to said microphone port of said unmodified radio.

15. (Currently Amended) The system according to claim 1 wherein said computer system for receiving comprises:

a microphone driver that is executing within said computer system converting said input analog signal to a file, said file being in a standard voice file format;

~~said~~ a first application constantly monitoring inputs received from said microphone;

said first application detecting a receipt of said file; and

wherein said computer system for encrypting comprises in response to a detection by said first application of said receipt of said file, said first application encrypting said file to form said encrypted voice file by utilizing a public key that is part of a public key/private key pair assigned to said computer system.

16. (Previously Presented) The system according to claim 11, further comprising:

a second conventional radio, said second conventional radio being incapable of encrypting or decrypting signals, said second radio including a second microphone port that is configured to be coupled to a second conventional microphone and a second speaker port that is configured to be coupled to a second conventional speaker, said second radio remaining unmodified;

a second computer system coupled between said second speaker and said second unmodified radio, wherein outputs from said second radio are received first by said second computer system before being output to said second speaker, said second computer system being separate and apart from said second radio;

said second computer system for receiving an encrypted output from said second speaker port included within said second unmodified radio;

said second computer system for decrypting said encrypted output utilizing public key encryption to form a decrypted output; and

said second computer system for outputting said decrypted output from said second computer system to said second speaker.

17. (Previously Presented) The system according to claim 16, wherein said second computer system for receiving further comprises:

a second application that is executing within said second computer system constantly monitoring said second speaker port; and

said second application receiving said encrypted output from said second speaker port;

wherein said computer system for decrypting comprises said second application decrypting said encrypted output utilizing public key encryption.

18. (Canceled)

19. (Previously Presented) The system according to claim 17, further comprising:

said second computer system for obtaining a private key of said computer system; and

wherein said computer system for decrypting further comprises said second computer system for decrypting said encrypted output utilizing said private key.

20. (Previously Presented) The system according to claim 19, further comprising said computer system for exchanging said private key between said computer system and said second computer system prior to transmissions of radio signals.

21. (Previously Presented) A computer program product executing within a data processing system for securing radio transmissions utilizing a conventional radio, said computer program product on recordable-type media comprising the data processing system implemented steps of:

instruction means for providing a conventional radio, said conventional radio being incapable of encrypting or decrypting signals, said radio including a conventional microphone port that is configured to be coupled to a conventional microphone and a conventional speaker port that is configured to be coupled to a conventional speaker, said radio remaining unmodified;

instruction means for providing a computer system coupled between a microphone and said radio, wherein inputs into said radio are received first by said computer system, said computer system being separate and apart from said radio;

instruction means for receiving, within said computer system, an input analog signal from said microphone;

instruction means for encrypting, within said computer system, said input analog signal utilizing public key encryption to form an encrypted voice file;

instruction means for passing said encrypted voice file from said computer system to said microphone port that is included within said unmodified radio; and

instruction means for transmitting said encrypted voice file utilizing said unmodified radio, wherein radio transmissions from said radio are secured.

22. (Original) The product according to claim 21, further comprising instruction means for encrypting, within said computer system, said input analog signal utilizing a key pair, said key pair including a public key and a private key.

23. (Original) The product according to claim 22, further comprising instruction means for encrypting, within said computer system, said input analog signal utilizing said public key.

24. (Previously Presented) The product according to claim 21, wherein the instruction means for receiving are within a first application executing within said computer system, said input analog signal from said microphone;

wherein said instruction means for encrypting utilize public key encryption to form said encrypted voice file;

wherein said instruction means for passing comprises instruction means for passing said encrypted voice file from said first application to said microphone port of said unmodified radio.

25. (Currently Amended) The product according to claim 21 wherein said instruction means for receiving comprises:

instruction means for converting, by a microphone driver that is executing within said computer system, said input analog signal to a file, said file being in a standard voice file format;

instruction means for constantly monitoring, by ~~said~~ a first application, inputs received from said microphone; and

instruction means for detecting, by said first application, a receipt of said file;

wherein said instruction means for encrypting comprises in response to a detection by said first application of said receipt of said file, instruction means for encrypting, by said first application, said encrypted voice file utilizing a public key that is part of a public key/private key pair assigned to said computer system to form said encrypted voice file.

26. (Previously Presented) The product according to claim 21, further comprising:

instruction means for providing a second conventional radio, said second conventional radio being incapable of encrypting or decrypting signals, said radio including a microphone port that is configured to be coupled to a conventional microphone and a speaker port that is configured to be coupled to a conventional speaker, said radio remaining unmodified;

instruction means for providing a second computer system coupled between said second speaker and said second unmodified radio, wherein outputs from said second radio are received first by said second computer system before being output to said second speaker, said second computer system being separate and apart from said second radio;

instruction means for receiving, within said second computer system, an encrypted output from said second speaker port included within said second unmodified radio;

instruction means for decrypting, within said second computer system, said encrypted output utilizing public key encryption to form a decrypted output; and

instruction means for outputting said decrypted output from said second computer system to said second speaker.

27. (Previously Presented) The product according to claim 26, wherein said instruction means receiving, within said second computer system further comprises:

instruction means for constantly monitoring, by a second application that is executing within said second computer system, said second speaker port; and

instruction means for receiving, by said second application, said encrypted output from said second speaker port;

wherein said instruction means for decrypting comprises instruction means for decrypting, by said second application, said encrypted output utilizing public key encryption.

28. (Canceled)

29. (Previously Presented) The product according to claim 27, further comprising:

instruction means for obtaining, by said second computer system, a private key of said computer system; and

wherein said instruction means for decrypting further comprises instruction means for decrypting said encrypted output utilizing said private key.

30. (Previously Presented) The product according to claim 29, further comprising instruction means for exchanging said private key between said computer system and said second computer system prior to transmitting said encrypted voice file.